(/)

iboss Acceptable Use Policy

This Acceptable Use Policy ("AUP") applies to the use of the Company Property, offered by iboss, Inc. d/b/a iboss ("Company") to its customers (each, a "Customer") and end-users whose mobile devices, computers, or computer systems, whether corporate-owned or personal (BYOD),("Devices") have been registered with Company Property (each, an "End-User"). Capitalized terms used herein but undefined have the meanings given to such term in the Company's Terms of Service and End User License Agreement available at: www.iboss.com/terms-of-use(/terms-of-use).

This AUP describes certain functionalities of the Company Property as well as unacceptable practices and prohibited actions while using the Company Property. As a Customer and/or End-User of the Company Property, you acknowledge and agree that you have read, understood and agree to this AUP. As a Customer, you also acknowledge and agree that you will ensure that your End-Users and employees abide by this AUP and that you will be responsible for violations of this AUP by your End-Users and employees. Company reserves the right to modify this AUP at any time, notifying you either via e-mail, the Company Property or by posting a revised copy of this AUP on our website. You agree to review this AUP on a regular basis and remain in compliance at all times.

Company Property

Among other things, the Company Property enables Customers to control, manage and secure certain aspects and functionalities of Devices which have been registered with the Company (each, a "Registered Device"). For example, the Company Property enables Customers to:

1. Secure all aspects of Internet traffic including web filtering, SSL access, applications, bandwidth throttling/QoS, on/off-premise mobile security, and BYOD management tools.
2. Set restrictions on certain Registered Device functionalities, such as restrictions on use of camera features, Bluetooth, or WiFi.
3. Set and enforce policies for applications, such as blacklisted apps.
4. Set social media controls.
5. Monitor and secure SaaS data.
6. Wipe lost devices and monitor applications; and create compliance reports.

Company does not monitor the content that Customer or any End-User stores on and provides to others through the Company Property and any other material used by Customer and End-Users in connection with the Company Property (collectively, the "Customer Content"), nor does Company exercise any editorial control over the Customer Content. However, and without limiting anything in Section 6, Company reserves the right to remove any Customer Content from the Service that is, in Company's discretion, potentially illegal, a violation of intellectual property laws, or may subject Company to liability, or violate this AUP. Upon removal of the material, Company shall notify Customer of the removal of the Customer Content, as well as the reason for removal. In no instance shall Company be liable for the removal of the Customer Content.

Prohibited Uses

1. No Infringing, Illegal, Threatening, Defamatory, and Offensive Uses. Neither Customer or End-User may use the Company Property to violate any applicable laws, rules, or regulations issued or promulgated by any competent government authority, including the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030) and Electronic Communications Privacy Act (18 U.S.C. § 2510 et. seq). Without limiting the foregoing, neither Customer nor any End-User shall use the Company Property for, or in connection with, the following:

1. Theft or infringement of copyrights, trademarks, trade secrets, or other types of intellectual property.
2. Fraud, forgery, or theft or misappropriation of funds, credit cards, or personal information.
3. Export, re-export, or transfer restricted software, algorithms or other data in violation of applicable export control laws.
4. Deceptive practices such as posing as another service for the purposes of phishing or pharming.
5. Distributing any materials of a threatening or harmful nature, including without limitation threats of death or physical harm, or materials that are malicious, harassing, libelous, defamatory, or which facilitate extortion.
6. Distributing any offensive materials, including without limitation obscene, pornographic, indecent or hateful materials and materials which promote gambling or discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age.

2. Necessary Consents. Customer understands and agrees that: (i) the Company Property may be used for legal purposes only; (ii) Customer is solely responsible for obtaining all necessary and appropriate consents from End-Users to access, monitor, modify and use the Registered Devices via the Company Property; (iii) Customer shall not access, monitor, modify or use such Registered Devices via the Company Property without obtaining the prior written consent from each applicable End-User; and (iv) Customer shall not use the Company Property in any manner which exceeds the scope of any consents obtained pursuant to subparts "ii" and "iii".

3. BYOD. Customer shall not access the personal email accounts or other personal applications on any Registered Device which is the personal property of its End-User (a "BYOD Device"). Customer understands and agrees that BYOD Devices are the personal property of their respective End-Users, and as such will only access and use those applications and systems on each BYOD Device

to which Customer has prior written consent. In the event any BYOD Device is lost or stolen, Customer shall not delete or wipe any personal data, personal applications or other personal content of the applicable End-User via the Company Property, without the express written consent of such End-User to do so. In addition, Customer shall not monitor or track the physical movements of any End-User via their BYOD Device without the express consent of use End-User; provided, however, that Customer shall not monitor End-User's physical movements in violation of applicable law, including without limitation the National Labor Relations Act.

4. Security and Interference. Customer shall not use the Company Property to violate, attempt to violate, or knowingly facilitate the violation of the security or integrity of any network, electronic service, or other system that is accessible through, or in connection with, the Company Property. Customer shall not use the Company Property in a manner that interferes with any other party's ability to use and enjoy the Company Property, that interferes with Company's or its service partners' ability to provide the Company Property, or that otherwise may create legal liability for Company or its service partners in Company's sole discretion. Customer shall not use the Company Property to violate the acceptable use policy or terms of service of any other service provider, including, without limitation, any Internet service provider. Without limiting the foregoing, Customer shall not use the Company Property for, or in connection with, the following:

1. Hacking, cracking into, or otherwise using the non-public areas of the Company Property or any other system without authorization.
2. Unauthorized probes or port scans for vulnerabilities.
3. Unauthorized penetration tests, traffic that circumvents authentication systems or other unauthorized attempts to gain entry into any system.
4. Web crawling which is not restricted to a rate so as not to impair or otherwise disrupt the servers being crawled.
5. Unauthorized network monitoring or packet capture.
6. Forged or non-standard protocol headers, such as altering source addresses.
7. Flooding.
8. Denial of Service (DoS) attacks of any kind.
9. Distributing unauthorized data, malware, viruses, Trojan horses, spyware, worms, or other malicious or harmful code.
10. Operating network Company Property such as: open proxies; open mail relays; or open, recursive domain name servers.
11. Sharing or publishing content from the Company Property to cause, or have the consequence of causing, the user of the content to be in violation of the terms and this AUP.

5."Spam." Customer shall not use the Company Property for purposes of distributing e-mail "spam," bulk unsolicited instant messages, or any other form of unsolicited electronic communications distributed on a bulk basis to recipients with which Customer has no preexisting business or personal relationship. Additionally, Customer shall not use the Company Property to collect responses from spam. Customer shall not harvest, collect, gather or assemble information or data of users, including e-mail addresses, without their consent. Without limiting the foregoing, Customer shall not use the Company Property for, or in connection with, the following:

1. Sending pyramid schemes.

2. Sending chain letters.
3. Sending any mail in contravention of the CAN SPAM Act of 2003 or other applicable state or federal laws and regulations.
4. Altering or obscuring mail headers or assuming the identity of a sender without the explicit permission of that sender.

6. Copyright Policy. If Company receives a notification of claimed copyright or trademark infringement with regard to Customer Content, whereby the notification includes: a physical or electronic signature of the owner (or person authorized to act on behalf of the owner) of an exclusive right that is allegedly infringed; specific identification of the copyrighted, trademark or patented work claimed to have been infringed, or if multiple works are covered by a single notification, a list of each work claimed to have been infringed; information related to the work(s) reasonably sufficient for Company to promptly locate the work (e.g. title of work, URL location) within the Company Property; information reasonably sufficient to permit Company to directly contact the complaining party, such as a complete name and address, telephone number and/or email address; a statement that the complaining party has a good faith belief that use of the work(s) in the manner complained of is not authorized by the copyright owner, its agent or the law; a statement requesting that Company take a specific act with respect to the alleged infringement (e.g., removal, access restricted or disabled; and a statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed, then Company will take appropriate actions under the Digital Millennium Copyright Act and/or other applicable intellectual property laws, which may including disabling or removing the Customer Content from the Company Property and/or suspend or terminate the provision of the Company Property to Customer and withhold Customer Content until the matter has been fully resolved by all parties and such resolution has been submitted in writing to Company on terms mutually acceptable to Company, or if court action of legal jurisdiction determines otherwise.

7. Violations. If Customer becomes aware of any violation of this AUP by any third party, Customer shall promptly report such violation to Company.

8. Changes to Policy. This AUP is subject to occasional revision, and if Company makes any substantial changes to this AUP, Company will notify the Customer and/or prominently post notice of the changes on the Company website. Any material changes to this AUP will be effective upon the earlier of thirty (30) calendar days following the notice to Customer or thirty (30) calendar days following Company's posting of notice of the changes on the Company website. If Customer does not agree to any changes to this AUP, Customer must notify Company prior to the effective date of the changes. Continued use of the Company Property, following notice of such changes, shall indicate Customer's acknowledgement of such changes and agreement to be bound by the terms and conditions of such changes.

This Acceptable Use Policy was last revised on March 13, 2014.

The iboss Story

About Us(/about-us)
Leadership(/leadership)
Board(/board-of-directors)
Blog(//blog.iboss.com)
In the News(/in-the-news)
Press Releases(/press-releases)

Legal

Privacy Policy(/privacy-policy)
Terms of Use(/terms-of-use)
Acceptable Use Policy(/acceptable-use-policy)

Site Map

Site Map(/site-map)

Learn iboss

iboss University Overview(/iboss-university)
ISCP Certification(//www.iboss.com/iuniversity-iscp)
Expand Your Knowledge(//www.iboss.com/iuniversity-eyk)

Contact Support

Support Overview(/support)
Open a Ticket(http://support.iboss.com)
Activate iboss Pro(//www.iboss.com/phantomweb/action/activation/selectProduct?b=1)
Cloud Management(//www.iboss.com/phantomweb/action/enterprisemanagement/login)

North America:
877-742-6832 X3

International:
858-568-7051 X3

Contact Sales

Request Demo(//www.iboss.com/demo-request)
Request Evaluation(//www.iboss.com/eval-request)
Request Information(//www.iboss.com/info-request)

North America:
877-742-6832 X1
Contact local distributor or:

sales@iboss.com(mailto:sales@iboss.com)

International:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com(mailto:sales@iboss.com)

EMEIA:
+44 (0) 203 713 0471
Contact local distributor or:
emeia@iboss.com(mailto:emeia@iboss.com)